Please note: The privacy and security excerpts provided below were included as attachments to the Terms and Conditions received by Navigator recipients in 2017 as part of their Notice of Award and are meant to serve as an example only. The standards for any future Navigator awardees may be different.

Notice of Award: Standard Grant/Cooperative Agreement Terms and Conditions

26. Project and Data Integrity. Recipient shall protect the confidentiality of all project-related information that includes personally identifying information.

The Recipient shall assume responsibility for the accuracy and completeness of the information contained in all technical documents and reports submitted. The CMS Project Officer shall not direct the interpretation of the data used in preparing these documents or reports.

At any phase in the project, including the project's conclusion, the Recipient, if so requested by the CMS Project Officer, must deliver to CMS materials, systems, or other items used, developed, refined or enhanced in the course of or under the award. The Recipient agrees that CMS shall have a royalty-free, nonexclusive and irrevocable license to reproduce, publish, or otherwise use and authorize others to use the items for Federal government purposes.

Notice of Award: Program Terms & Conditions Attachment H

11. Navigator Oversight and Monitoring.

a. Recipient shall establish processes to monitor program activities for compliance with statutory, regulatory and grant requirements, including but not limited to compliance with the privacy and security requirements set forth in this document (Attachment H, Program Terms and Conditions) and in Attachments I and J.
b. Recipient is required to report to CMS any instance of suspected fraud, misconduct or non-compliance with statutory, regulatory or grant requirements on the part of staff or the organization as a whole.
c. Recipient should make contact information for the HHS OIG available to Consumers and to Recipient staff. For example, this could be done by posting this information in a public space or by including in educational materials distributed by Recipient.

19. Privacy and Security Compliance.

Definitions. Capitalized terms not otherwise specifically defined in this specific term and condition shall have the meaning set forth in Attachment J.

Recipient hereby acknowledges and agrees to accept and abide by the standards and implementation specifications set forth in this document (Attachment H, Program Terms and Conditions) and in Attachment I ("Privacy and Security Standards for Navigator Grant Recipients") when engaging in any Navigator Authorized Functions as defined below. Recipient is thereby bound to strictly adhere to the privacy and security standards, and to ensure that its Workforce that creates, collects, accesses, stores, maintains, discloses, or uses PII, is contractually bound to strictly adhere to those standards and implementation specifications.

Navigator Authorized Functions. Recipient may create, collect, handle, disclose, access, maintain, store, and/or use PII of Consumers, only to perform:

a. the required duties described in section 1311(i)(3) of the Affordable Care Act, 45 CFR 155.210 and 155.215, and the Cooperative Agreement to Support Navigators in Federally-Facilitated and State Partnership Marketplaces Funding Opportunity Announcement ("Navigator FOA"), as well as in Recipient's approved work and project plans;
b. functions related to carrying out additional obligations as may be required under applicable state law or regulation, provided that (1) such a state requirement does not prevent the application of the provisions of title I of the Affordable Care Act within the meaning of section 1321(d) of the Affordable Care Act, and (2) Recipient notifies Consumers, in advance, in writing, that creation, collection, handling, disclosure, access, maintenance, storage, and/or use of their PII might be required under applicable state law or regulations. Recipient should provide the required notification through the authorization obtained in accordance with 45 CFR 155.210(e)(6); and
c. other functions authorized under 45 CFR 155.210 and 155.215, and such other functions that may be approved by CMS in writing from time to time.

The required duties that are most likely to involve the creation, collection, handling, disclosure, access, maintenance, storage and/or use of PII of Consumers include the following:

- Provide information and services in a fair, accurate, and impartial manner, which includes: providing information that assists consumers with submitting the eligibility application; clarifying the distinctions among health coverage options, including

QHPs; and helping consumers make informed decisions during the health coverage selection process. Such information must acknowledge other health programs;

- Facilitate selection of a QHP;
- Provide referrals to any applicable office of health insurance consumer assistance or health insurance ombudsman established under Section 2793 of the PHS Act, or any other appropriate State agency or agencies, for any enrollee with a grievance, complaint, or question regarding their health plan, coverage, or a determination under such plan or coverage;
- Provide information in a manner that is culturally and linguistically appropriate to the needs of the population being served by the Marketplace, including individuals with limited English proficiency, and ensure accessibility and usability of Navigator tools and functions for individuals with disabilities in accordance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act;
- Comply with the authorization requirements set forth in 45 CFR 155.210(e)(6) and summarized below; and
- Provide information to Consumers about the full range of QHP options and insurance affordability programs for which they are eligible, in accordance with 155.215(a)(1)(iii).

Other Required Duties: Recipient must also maintain expertise in eligibility, enrollment, and program specifications and conduct public education activities to raise awareness about the Marketplace; however, it is not expected or required that Recipient create, collect, handle, disclose, access, maintain, store and/or use PII of Consumers for this function. To the extent that Recipient does so, it must comply with all of the provisions of this specific term and condition, as well as Attachments H, I, and J that apply to Recipient's activities.

PII Received. Subject to these terms and conditions of this Notice of Award and applicable laws, in performing the tasks contemplated under this award, Recipient may create, collect, disclose, access, maintain, store, and/or use the following data and PII from Consumers:

Access to or enrollment in employer or other health coverage
American Indian/Alaska Native status
APTC percentage and amount applied
Auto disenrollment information
Applicant Name
Applicant Address
Applicant Birthdate
Applicant Telephone number
Applicant Email
Applicant spoken and written language preference
Applicant Medicaid Eligibility indicator, start and end dates

Applicant Children's Health Insurance Program eligibility indicator, start and end dates
Applicant QHP eligibility indicator, start and end dates
Applicant APTC percentage and amount applied eligibility indicator, start and end dates
Applicant household income
Applicant Maximum APTC amount
Applicant Cost-sharing Reduction (CSR) eligibility indicator, start and end dates
Applicant CSR level
Applicant QHP eligibility status change
Applicant APTC eligibility status change
Applicant CSR eligibility status change
Applicant Initial or Annual Open Enrollment Indicator, start and end dates
Applicant Special Enrollment Period eligibility indicator and reason code
Citizenship status
Contact Name
Contact Address
Contact Birthdate
Contact Telephone number
Contact Email
Contact spoken and written language preference
Enrollment group history (past six months)
Enrollment type period
FFE Applicant ID
FFE Member ID
Gender
Immigration document type and document numbers
Issuer Member ID
Membership in a Federally recognized tribe
Net premium amount
Premium Amount, start and end dates
Pregnancy indicator
Race/ethnicity
Sex
Special enrollment period reason
Subscriber Indicator and relationship to subscriber
Social Security Number
Tax filing status (tax filer, tax dependent, non-filer)
Tobacco use indicator and last date of tobacco

Storing PII. To the extent that Recipient maintains or stores PII, it must agree to comply with all provisions of these terms and conditions that apply to the maintenance or storage of PII.

Privacy and Security Obligations of Recipient. As a condition of this grant, Recipient will implement and comply with all Marketplace privacy and security standards set forth in these terms and conditions.

Authorization Requirement. Prior to creating, collecting, handling, disclosing, accessing, maintaining, storing, and/or using any PII from Consumers, Recipient must obtain the authorization required under 45 CFR 155.210(e)(6), to ensure that Consumers:

- are informed of the functions and responsibilities of Navigators, including that Navigators are not acting as tax advisers or attorneys when providing assistance as Navigators and cannot provide tax or legal advice within their capacity as Navigators;
- provide authorization in a form and manner as determined by CMS prior to a Navigator's obtaining access to their PII, and that the Navigator maintains a record of the authorization provided in a form and manner as determined by CMS, for no less than six years, unless a different and longer retention period has already been provided under other applicable Federal law; and
- may revoke this authorization at any time.

A model template authorization form developed by CMS will be provided separately to all Recipients for their optional use.

This authorization is separate and distinct from any informed consent obtained pursuant to section 2(b) of Attachment I of this Agreement. Recipient should ensure that a record of the authorization provided is maintained in a manner consistent with the privacy and security standards set forth in this document (Attachment H, Program Terms and Conditions) and in Attachment I.

Collection of PII. Except for collections, uses or disclosures that are specifically authorized by Consumers in accordance with Section 2(b) of Attachment I, PII collected from Consumers may be used only for the Navigator Authorized Functions specified in this term and condition.

Ability of Consumer to Limit Collection and Use. Recipient agrees to allow the Consumer to limit the Recipient's creation, collection, use, maintenance, storage, and disclosure of their PII to the sole purpose of obtaining Recipient's assistance for Federally-facilitated Marketplace purposes, and for performing Navigator Authorized Functions specified in this term and condition.

Applicability to Workforce. Recipient must impose the same standards described in this specific term and condition and in Attachments H and I on all Workforce members working with the Recipient on this grant program.

Survival. Recipient covenants and agrees to destroy all PII of Consumers in its possession at the end of the record retention period required under this specific term and condition and in

Attachments H and I. Recipient's duty to protect and maintain the privacy and security of PII, as provided for in accordance with this specific term and condition, and Attachments H and I, shall continue in full force and effect until such PII is destroyed and shall survive the termination or withdrawal of the Navigator Recipient and/or expiration of this award.

20. Sub-Recipients' Compliance with Privacy and Security Requirements. Any and all Sub-Recipients are also required to adhere to all privacy and security requirements outlined in this document (Attachment H, Program Terms and Conditions) and in Attachment I.

23. PII Authorization. Recipient may not create, collect, handle, disclose, access, maintain, store, and/or use the PII (as defined in Attachment J) of any Consumers until it has drawn down funds and accepted the terms and conditions of this award.

Notice of Award: Program Terms & Conditions
Attachment I

PRIVACY AND SECURITY STANDARDS FOR NAVIGATOR GRANT RECIPIENTS

These standards and implementation specifications are established in accordance with Section 1411(g) of the Affordable Care Act (42 U.S.C. § 18081(g)) and 45 CFR 155.260. As used in this Attachment, all terms used herein carry the meanings assigned in Attachment J of the Notice of Award.

Navigator Grant Recipient ("Recipient"), and any members of Recipient's Workforce who are certified by CMS to carry out Navigator duties, or who otherwise have access to the PII of consumers who seek the Recipient's assistance, must adhere to the following privacy and security standards and implementation specifications in performing the Navigator Authorized Functions defined in Attachment H of the Notice of Award.

(1) Privacy Notice Statement. Prior to collecting PII or other information from Consumers for the purpose of fulfilling a Navigator Authorized Function, Recipient must provide Consumers with a privacy notice statement. The privacy notice statement must be in writing and must be provided on, or simultaneously with, any electronic and/or paper form the Recipient will use to gather and/or request PII or other information from Consumers. The privacy notice statement must also be prominently and conspicuously displayed on the Recipient's public facing Web site, if applicable, if the Recipient will gather or request PII or other Consumer information through that Web site.

a. Privacy Notice Statement Requirements.

i. The privacy notice statement must be written in plain language and, to the extent possible, provided in a manner that is accessible and timely to people living with disabilities and with limited English proficiency.

ii. The statement must contain at a minimum the following information:

1. A description of the information to be collected;
2. The purpose for which the information is being collected;
3. The intended use(s) of the information;
4. To whom the information may be disclosed, for what purposes, and how a record of any disclosures may be requested from the Recipient;
5. What, if any, notice or opportunities for consent will be provided regarding the collection, use or disclosure of the information;
6. How the information will be secured;
7. Whether the request to collect information is voluntary or mandatory under the applicable law;
8. Effects of non-disclosure if a Consumer chooses not to provide the requested information;
9. Any rights the person may have under state or federal laws relevant to the protection of the privacy of an individual; and
10. Information on how to file complaints with CMS and the Recipient related to the Recipient's activities in relation to the information.

iii. The Recipient shall maintain its privacy notice statement content by reviewing and revising it as necessary on an annual basis, at a minimum, and before or as soon as possible after any change to its privacy policies and procedures.

b. Notwithstanding the general requirement above to provide a written privacy notice statement prior to collecting PII or other information from Consumers, this provision does not require Recipients to provide a written privacy notice statement to Consumers prior to collecting a Consumer's name, physical address, e-mail address, or telephone number, so long as such information will be used solely for the purpose of making subsequent contact with the Consumer to conduct a Navigator Authorized Function or sending to the consumer educational information that is directly relevant to Navigator Authorized Functions. Nonetheless, with regard to such names, physical addresses, e-mail addresses, or telephone numbers, Recipients still must comply with all privacy and security

standards and requirements outlined in the CMS Navigator Grant Terms and Conditions.

(2) Permissible Uses and Disclosures of PII. The Recipient and members of Recipient's Workforce who are certified by CMS to carry out Navigator duties may create, collect, disclose, access, maintain, store, and use PII from Consumers only for Navigator Authorized Functions identified in Attachment H, unless the Recipient obtains informed consent as described in Section 2(b) of this Attachment I.

a. Authorization:

i. Prior to creating, collecting, disclosing, accessing, maintaining, storing, or using any Consumer PII to perform a Navigator Authorized Function, the Recipient must obtain the authorization required by 45 CFR 155.210(e)(6), This authorization is separate and distinct from the informed consent referenced in Section 2(b) below;

ii. Recipients must maintain a record of the authorization provided for a period of no less than six (6) years, unless a different and longer retention period has already been provided under other applicable Federal law; and

iii. Recipients must permit the Consumer to revoke the authorization at any time.

b. Informed Consent:

i. Recipients must obtain informed consent from Consumers for any creation, collection, use or disclosure of information that is not authorized under these Terms and Conditions. Such informed consent must be in writing, signed by the consenting party, and subject to a right of revocation.

ii. Recipients are prohibited from denying information or assistance to persons or entities that do not wish to grant consent for any creation, collection, use or disclosure of Consumer information that is not authorized under these Terms and Conditions.

iii. Informed consent must:

1. Be provided in specific terms and in plain language;
2. Identify who will obtain access to the Consumer's information under the terms of the informed consent;
3. Describe the purpose for which the informed consent is being obtained;

4. Explain what information the Recipient will use or disclose to a specific recipient(s);
5. Provide notice of a Consumer's ability to revoke the consent at any time; and
6. Include an expiration date or event, unless effectively revoked in writing by the Consumer before that date or event.

iv. Informed consent documents must be appropriately secured and retained for no less than six (6) years, unless a different and longer retention period has already been provided under other applicable Federal law.

(3) Limitations on creation, collection, disclosure, access, maintenance, storage, and use.

a. Permissible creation and use of PII.

Other than in accordance with the informed consent procedures outlined above, the Recipient shall only create, collect, disclose, access, maintain, store, or use PII it receives in its capacity as a Navigator Grant Recipient:

i. In accordance with the privacy notice statement referenced in Section (1) above; and/or
ii. In accordance with the Navigator Authorized Functions.

b. Prohibited requests for, collections, or uses of PII.

The Recipient shall not:

i. request or require a social security number, information regarding citizenship, status as a national, or immigration status for any individual who is not seeking coverage for himself or herself on an application;
ii. request information from or concerning any individual who is not seeking coverage for himself or herself, unless the information is necessary for the eligibility determination for enrollment in a Qualified Health Plan or Insurance Affordability Programs for those seeking coverage, or is required as part of a SHOP employer application under 45 C.F.R. §155.730. Such necessary information may include information on individuals who are in an individual's tax household or who live with an individual applying for coverage, including contact information, addresses, tax filing status, income and deductions, access to employer-sponsored coverage, familial or legal relationships, American Indian or Alaska Native status, or pregnancy status; or

iii. use a Consumer's or any other individual's PII to discriminate against them, such as by refusing to assist individuals who have significant or complex health care needs.

c. Accounting for Disclosures. Except for those disclosures that are necessary to carry out Navigator Authorized Functions, Recipients that maintain and/or store PII shall maintain an accounting of any and all disclosures of PII. The accounting shall:

i. Contain the date, nature, and purpose of such disclosures, and the name and address of the person or agency to whom the disclosure is made;

ii. Be retained for at least six (6) years after the disclosure, or the life of the record, whichever is longer; and

iii. Be available to CMS, or the Consumer who is the subject of the record, upon request.

(4) Safeguarding PII.

a. Recipients must ensure that PII is protected with reasonable operational, administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure. Specifically, Recipient is required to establish and implement operational, technical, administrative and physical safeguards that are consistent with any applicable laws and ensure that:

i. PII is only used by or disclosed to those authorized to receive or view it;

ii. PII is protected against any reasonably anticipated threats or hazards to the confidentiality, integrity, and availability of such information;

iii. PII is protected against any reasonably anticipated uses or disclosures of such information that are not permitted or required by law; and

iv. PII is securely destroyed or disposed of in an appropriate and reasonable manner and in accordance with record retention requirements under the Terms and Conditions.

b. Recipients must monitor, periodically assess, and update the security controls and related system risks to ensure the continued effectiveness of those controls.

c. Recipients must develop and utilize secure electronic interfaces when transmitting PII electronically.

(5) Incident and Breach Reporting Requirements.

a. Reporting. Recipients must implement and comply with Breach and Incident handling procedures that are consistent with CMS' Risk Management Handbook Standard 7.1 Incident Handling and Breach Notification[1] and memorialized in the Recipient's own policies and procedures. Such policies and procedures must be in writing and:

i. Identify the Recipient's Designated Privacy Official, if applicable, and/or identify other personnel authorized and responsible for reporting and managing Incidents or Breaches to CMS;

ii. Address how to identify Incidents;

iii. Determine if personally identifiable information (PII) is involved in the Incidents;

iv. Require all members of Recipient's Workforce to report all potential Incidents or Breaches to Recipient;

v. Require reporting any Incident or Breach of PII to the CMS IT Service Desk by telephone at (410) 786-2580 or 1-800-562-1963 or via email notification at cms_it_service_desk@cms.hhs.gov within **one hour** of discovery of the Incident or Breach;

vi. Require the completion of the CMS Security Incident Report, a copy of which is attached hereto as Attachment K or a copy of which may be found at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/CMS1253654.html?DLPage=2&DLSort=0&DLSortDir=ascending;

vii. Provide details regarding the identification, response, recovery, and follow-up of Incidents and Breaches; and

[1] Available at http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/RMH_VIII_7-1_Incident_Handling_Standard.pdf

viii. Require the Recipient's Designated Privacy Official and/or other authorized personnel to be available to CMS upon request.

b. Members of Recipient's Workforce must comply with Navigator Awardee Organization's Breach and Incident handling procedures.

c. Cooperation. Recipients must cooperate with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII; the provision of a formal response to an allegation of unauthorized PII use, reuse or disclosure; and/or the submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures.

(6) Training and Awareness Requirements. The Recipient shall develop role-based training and awareness programs for members of its Workforce who are certified by CMS to carry out Navigator duties or who otherwise have access to the PII of consumers who seek the Recipient's assistance. Recipient shall require such members of its Workforce to participate in such training and awareness programs. Specifically, the Recipient must require such members of its Workforce to successfully complete privacy and security training that is specifically tailored and relevant to their work duties and level of exposure to PII, and prior to when they assume responsibility for/have access to PII, and members of Recipient's Workforce must successfully complete such training prior to assuming responsibility for/having access to PII.

(7) Standard Operating Procedures Requirements. The Recipient shall incorporate the privacy and security standards and implementation specifications required under this Attachment I, where appropriate, in its standard operating procedures that are associated with the functions authorized under Navigator Terms and Conditions involving the creation, collection, disclosure, access, maintenance, storage, or use of PII. Members of Recipient's Workforce who are certified by CMS to carry out Navigator duties, or who otherwise have access to the PII of consumers who seek the Recipient's assistance, must comply with these standard operating procedures. The Recipient's standard operating procedures:

a. Must be written in plain language and be available to all of the Recipient's Workforce;

b. Must ensure the Recipient's cooperation with CMS in resolving any Incident or Breach, including (if requested by CMS) the return or destruction of any PII files it received under the Navigator Terms and Conditions; the provision of a formal response to an allegation of unauthorized PII use, reuse or disclosure; and/or the

submission of a corrective action plan with steps designed to prevent any future unauthorized uses, reuses or disclosures; and

c. Must be designed and implemented to ensure the Recipient and its Workforce comply with the standards and implementation specifications contained herein, and must be reasonably designed, taking into account the size and the type of activities that relate to PII undertaken by the Recipient, to ensure such compliance.

(8) Required Monitoring of Security Controls. Recipient must monitor, periodically assess, and update its security controls and related system risks to ensure the continued effectiveness of those controls.

(9) Required Flow-Down of Privacy and Security Agreements. Recipient must bind, in a signed writing, any members of Recipient's Workforce who are certified by CMS to carry out Navigator duties, and any Downstream Entities to the same privacy and security standards and obligations contained in this Attachment I.

(10) Compliance with the Internal Revenue Code. If any "return information," as defined in section 6103(b)(2) of the Internal Revenue Code (the Code), is accessed or used by Recipient, it must be kept confidential and disclosed, used, and maintained only in accordance with section 6103 of the Code.

(11) Penalties for improper use and disclosure of information. Recipient acknowledges that any person who knowingly and willfully uses or discloses information in violation of section 1411(g) or 1411(h) of the Affordable Care Act will be subject to a civil money penalty, consistent with the bases and process for imposing civil penalties specified at 45 C.F.R. 155.206 and/or 155.285, in addition to other penalties that may be prescribed by law.

Notice of Award: Program Terms and Conditions
Attachment J

This Attachment defines terms that are used in Attachments H, I, and J.

DEFINITIONS

(1) **Affordable Care Act (ACA)** means the Patient Protection and Affordable Care Act of 2010 (Public Law 111-148), as amended by the Health Care and Education Reconciliation Act of 2010 (Public Law 111-152), which are referred to collectively as the Affordable Care Act.

(2) **Advance Payments of the Premium Tax Credit (APTC)** has the meaning set forth in 45 CFR 155.20.

(3) **Applicant** has the meaning set forth in 45 CFR 155.20.

(4) **Authorized Function** means a task performed by a Non-Exchange Entity that the Non-Exchange Entity is explicitly authorized or required to perform based on applicable law or regulation, and as enumerated in these Terms and Conditions.

(5) **Authorized Representative** means a person or organization meeting the requirements set forth in 45 CFR 155.227.

(6) **Breach** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for anything other than an authorized purpose.

(7) **CCIIO** means the Center for Consumer Information and Insurance Oversight within the Centers for Medicare & Medicaid Services (CMS).

(8) **CMS** means the Centers for Medicare & Medicaid Services.

(9) **Consumer** means an Applicant, Enrollee, Qualified Individual, Qualified Employer, or Qualified Employee, and (if applicable) their legal or Authorized Representatives, or any individual who presents himself or herself for assistance related to an Authorized

Function from a Non-Exchange Entity, or who is offered assistance related to an Authorized Function by a Non-Exchange Entity, as applicable.

(10) **Cost-sharing Reduction (CSR)** has the meaning set forth in 45 CFR 155.20.

(11) **Designated Privacy Official** means a contact person or office responsible for receiving complaints related to Breaches or Incidents, able to provide further information about matters covered by the Non-Exchange Entity privacy notice statement required by Section (1) of Attachment I, responsible for the development and implementation of the privacy and security policies and procedures of the Non-Exchange Entity, and responsible for ensuring the Non-Exchange Entity has in place appropriate safeguards to protect the privacy and security of PII.

(12) **Downstream Entity** means any party that enters into an agreement with Recipient or with another Downstream Entity for purposes of providing services related to the Navigator grant. The term "downstream entity" is intended to reach the entity that directly provides services to Consumers.

(13) **Enrollee** has the meaning set forth in 45 CFR 155.20.

(14) **Exchange** has the meaning set forth in 45 CFR 155.20. The term "Exchange" is commonly used to refer to the American Health Benefit Exchanges that are described at Affordable Care Act section 1311(b) and defined at 45 C.F.R. §155.20**.**

(15) **Federally-facilitated Exchange (FFE)** means an **Exchange** established by HHS and operated by CMS under Section 1321(c)(1) of the ACA for individual or small group market coverage.

(16) **HHS** means the U.S. Department of Health & Human Services.

(17) **Incident**, or **Security Incident**, has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017) and means an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

(18) **Information** means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

(19) **Insurance Affordability Program** means a program that is one of the following:

(1) A State Medicaid program under title XIX of the Social Security Act.

(2) A State children's health insurance program (CHIP) under title XXI of the Social Security Act.

(3) A State basic health program established under section 1331 of the Affordable Care Act.

(4) A program that makes coverage in a Qualified Health Plan through the Exchange with Advance Payments of the Premium Tax Credit established under section 36B of the Internal Revenue Code available to Qualified Individuals.

(5) A program that makes available coverage in a Qualified Health Plan through the Exchange with Cost-sharing Reductions established under section 1402 of the Affordable Care Act.

(20) **Navigator** has the meaning set forth in 45 CFR 155.20.

(21) **Non-Exchange Entity** has the meaning at 45 CFR 155.260(b), and includes but is not limited to Navigator grant recipients, and their staff and volunteers who are certified by CMS to carry out Navigator duties.

(22) **OMB** means the federal government's Office of Management and Budget.

(23) **Personally Identifiable Information (PII)** has the meaning contained in OMB Memoranda M-17-12 (January 3, 2017), and refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

(24) **Qualified Employee** has the meaning set forth in 45 CFR 155.20.

(25) **Qualified Employer** has the meaning set forth in 45 CFR 155.20.

(26) **Qualified Health Plan (QHP)** has the meaning set forth in 45 CFR 155.20.

(27) **Qualified Individual** has the meaning set forth in 45 CFR 155.20.

(28) **Security Control** means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(29) **State Partnership Exchange (SPE)** means a type of FFE in which a State engages actively with the federal government in the operation of certain aspects of the FFE.

(30) **Subaward** means an award provided by a pass-through entity to a subrecipient for the subrecipient to carry out part of a Federal award received by the pass-through entity. It does not include payments to a contractor or payments to an individual that is a beneficiary of a Federal program. A subaward may be provided through any form of legal agreement, including an agreement that the pass-through entity considers a contract.

(31) **Subrecipient** means a non-Federal entity that receives a subaward from a pass-through entity to carry out part of a Federal program; but does not include an individual that is a beneficiary of such program. A subrecipient may also be a recipient of other Federal awards directly from a Federal awarding agency. For purposes of these terms and conditions, subawardee and subrecipient retain the same meaning.

(32) **Web** means the World Wide Web.

(33) **Workforce** means a Non-Exchange Entity's or sub-recipients' employees, agents, contractors, subcontractors, officers, directors, agents, representatives, and any other individual who may create, collect, disclose, access, maintain, store, or use PII in the performance of his or her duties.

Notice of Award: Program Terms and Conditions
Attachment K

Computer Security Incident Report

Date/Time:

Incident Tracking Number		

**** = Required information***

Reporting Individual Contact Information			

Impacted User Contact Information			

Incident Category			
	PII | PHI | FTI Incident (Section A)		CAT 5 Scans/Probes (*Section G*)
	CAT 0 Exercise/Network Defense Testing (*Section B*)		CAT 6 Investigations (*Section H*)
	CAT 1 Unauthorized Access (*Section C*)		CAT 7 Other (*Section I*
	CAT 2 Denial of Service (*Section D*)		CAT 8 Lost/Stolen Asset (*Section J)*
	CAT 3 Malicious Code (*Section E*)		CAT 99 Non-Incident (*Section k*)
	CAT 4 Improper Usage (*Section F*)		

Impact Classification*		
		HIGH - Organization has lost the ability to provide all critical services to all system users
		MEDIUM - Organization has lost the ability to provide a critical service to a subset of system users.
		LOW - Organization has experienced a loss of efficiency, but can still provide all critical services to all users with minimal effect on performance.
		NONE - Organization has experienced no loss in ability to provide all services to all users.
		CLASSIFIED - The confidentiality of classified information was compromised.
		PROPRIETARY - The confidentiality of unclassified proprietary information, such as protected critical infrastructure (PCCII), intellectual property, or trade secrets was compromised.
		PRIVACY - The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised.
		INTEGRITY - The necessary integrity of information was modified without authorization.
		NONE - No information was exfiltrated, modified, deleted, or otherwise compromised.
		REGULAR - Time to recovery is predictable with existing resources.
		SUPPLEMENT - Time to recovery is predictable with additional resources.
		EXTENDED - Time to recovery is unpredictable; additional resources and outside help are needed.
		NOT RECOVERABLE - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
		NOT APPLICABLE - Incident does not require recovery.

Threat Vector Identification*		
	UNKNOWN	Cause of attack is unidentified
	ATTRITION	An attack that employs brute force methods to compromise, degrade, or destroy systems, networks or services
	WEB	An Attack executed from a website or web-based application.
	E-MAIL	An attack executed via e-mail message or attachment.
	EXTERNAL/REMOVABLE MEDIA	An attack executed from removable media or a peripheral device.
	IMPERSONATION / SPOOFING	An attack involving replacement of legitimate content/services with a malicious substitute.
	IMPROPER USAGE	Any incident resulting from violation of an organization's acceptable usage policies by an authorized user, excluding the above categories.
	LOSS OR THEFT OF EQUIPMENT	The loss or theft of a computing device or media used by the organization.
	OTHER	An attack does not fit into any other vector.

Section A: PII / PHI / FTI Breach			
	Document Theft		Improper Usage
	Hardware / Media Theft		Unintended manual Disclosure
	Document Loss		Unintended Electronic Disclosure
	Hardware / Media Loss		Hacking or IT Incident
	Document Lost in Transit		Document sent to Wrong Address
	Hardware / Media Lost in Transit		

Number and Description of PII / PHI / FTI Lost or Compromised			
	Exact Number of PII:		Check Here if Number is Unknown:

Section B: Exercise / Testing (CAT 0)		
Name:		
Phone:		

Section C: Unauthorized Access (CAT 1)

Section E: Malicious Code (CAT 3)				
	Worm			
	Virus			
	Buffer Overflow		Cleaned	
	Denial of Service		No Action	
	Other			
		Yes		No

Section F: Improper Usage (CAT 4)	
	(P2P) File Sharing
	Instant Messenger
	Remote Access
	Unapproved Software
	Other

Section G: Scans / Probes / Attempted Access (CAT 5)		

Section H: Investigation (CAT 6)		

Section I: Other (CAT 7)		